WatchGuard® XCS v9.2 Update 4 Release Notes

WatchGuard XCS Build	121105
Revision Date	November 15, 2012

Introduction

WatchGuard® is pleased to announce the release of WatchGuard XCS v9.2 Update 4. This update release provides several new features and enhancements, and resolves several issues reported by WatchGuard customers.

New Features and Enhancements

The WatchGuard XCS v9.2 Update 4 release provides these new features and enhancements.

Content Scanning Internationalization Support

The WatchGuard XCS now supports non-Western languages when you use the Content Scanning feature on messages and files that use international Unicode character sets. This includes languages such as Chinese (traditional and simplified), Japanese, Korean, Russian, and Greek. Right-to-left languages such as Hebrew and Arabic are not supported. In addition, accented characters in Western languages such as German, Norwegian, and French are now processed and displayed properly.

To enable Content Scanning internationalization, select **Security > Content Control > Content Scanning**, then select the **Enable international document capability** check box.

If internationalized content scanning support is enabled, the system converts all uploaded dictionary contents to UTF-8 for Content Scanning, and the dictionary contents are displayed in UTF-8 format on the Dictionaries page. Your web browser must be configured to display the UTF-8 character set to properly view the contents of the dictionary file.

End-User Agreement for Login Page

A new End-User Agreement option allows you to display a disclaimer on the WatchGuard XCS login page that a user must accept before they can log in. This option applies to logins by administrators, tiered administrators, Spam Quarantine/Trusted Senders, and WebMail users. You can customize the default End-User Agreement text to reflect the specific acceptable use or legal policies of your organization. To enable and customize the End-User Agreement, select **Configuration > Miscellaneous > Customization**.

Download a List of Imported Directory Users

You can now download a list of users imported to the XCS via LDAP. You can use the downloaded list to examine the email addresses of imported and mirrored users to verify the stored information for recipient verification. To download a list of imported users, select **Configuration > LDAP > Directory Users**, and then click **Download Imported Users**.

Embed Fonts Option for PDF Reports

A new **Embed Fonts** option has been added that allows you to enable or disable the embedding of fonts directly into a PDF report. This option is enabled by default and improves compatibility for different types of PDF viewers, but significantly increases the size of PDF reports. Disable this option to reduce the size of PDF reports. Your PDF viewer will download any fonts required to view reports that do not have embedded fonts. To configure the Embed Fonts option, select **Configuration > Miscellaneous > Reports**.

SSL Renegotiation Option for TLS Sessions

A new **Allow SSL Renegotiation** option has been added to the TLS Encryption configuration page that allows SSL renegotiation after a TLS session has been established between the XCS and another mail server. This option is enabled by default. You can disable this option to mitigate SSL renegotiation denial-of-service attacks and avoid issues with standard security scans, but this can cause interoperability issues with some types of TLS connections. You should allow SSL renegotiation if connection problems with your TLS sessions occur. To configure the SSL renegotiation option, select **Security > Encryption > TLS**.

Private Root CA Certificate Bundle Support

The Root CA (Certificate Authority) certificate bundle file is used by the system to validate certificates issued by well-known Root Certificate Authorities. For secure sites that want to utilize a private Root CA certificate bundle, you can now upload a new file on the **Administration > System > SSL Certificates** page. Click **Advanced** for additional options that allow you to manage the Root CA bundle file. To download a copy of your current Root CA bundle file, click **Download**. To upload a new Root Certificate Authority bundle, click **Browse** to select your file, then click **Upload**. When the file is installed, the new Root CA bundle will take effect for TLS sessions and the use of certificates with the Web Proxy.

Ignore HTTP/1.1 Header Option for Web Proxy

A new **Ignore HTTP/1.1 Expect Header** option has been added to allow HTTP/1.1-based web applications to work properly through the WatchGuard XCS Web Proxy. This option ignores any *Expect: 100-continue* options in a web response from a client. To configure this option, select **Configuration > Web > HTTP/S Proxy > Show Advanced Options**.

Tiered Admin User Profile Page

Tiered administrators who do not have full admin privileges and do not have a local account (for example, on a clustered system) can now update their user profile and change their password from a User Profile page. To access the User Profile page, log in to the system, and from the tiered administrator drop-down list of options, select **User Profile**.

Resolved Issues

This release contains a number of defect fixes for issues reported by WatchGuard customers. See the Resolved Issues section below for a complete list of resolved issues.

Before You Begin

Before you install this update release:

- Read the information in the Known Issues and Limitations section of these Release Notes.
- For more information about how to configure WatchGuard XCS, from the Web UI, select **Support > Online Manual**.
- The latest versions of the product documentation are available at www.watchguard.com/help/documentation.

Download Software

If Security Connection is enabled, the software update is downloaded automatically to your XCS device. The update is not automatically installed. You must manually install software updates on the **Software Updates** page. See the *Install the Software Update* section below for detailed instructions.

To download the software manually:

1. Go to http://www.watchguard.com/archive/softwarecenter.asp.
2. Log in to the WatchGuard Portal and click the **Articles & Software** tab.
3. Search to see all available **Software Downloads** articles and find the **WatchGuard XCS Software Downloads** article.
4. Select and download the WatchGuard XCS v9.2 Update 4 software. The file is called `xcs92_update_4.pf`.

Install the Software Update

To install this update release:

Back Up the WatchGuard XCS Configuration

1. Select **Administration > Backup/Restore > Backup and Restore.**
2. Select your backup method (**FTP**, **SCP**, or **Local Disk**), then click **Next**.
3. Select which information to back up. If you do not want to restore reporting data, clear the **Backup reporting db data** check box. We recommend you select all options.

   For the **FTP** and **SCP** methods, enter your server information.
4. Click **Next** to confirm your selections.
5. Click **Create backup now**.

Install the Software Update

1. Select **Administration > Software Update > Updates**.
2. If you use Security Connection, the software update already appears in the **Available Updates** section.

   If you manually downloaded your software update:

   - Click **Browse** and select the software update.
   - Click **Upload**.

3. In the **Available Updates** section, select the software update.
4. Click **Install**. The device will restart when the installation is complete.

> ***Note*** *The installation process can take several minutes to complete.*

To Install the Software Update in a Cluster

1. On all devices in the cluster, change the cluster run mode to **Standalone** mode.
2. Install the update on the **Primary**, and then restart the device.
3. Change the run mode of the **Primary** device from **Standalone** back to **Primary** mode.
4. Install the update on the **Secondary**, and then restart the device.
5. Change the run mode of the **Secondary** system from **Standalone** back to **Secondary** mode.
6. Install the update on any **Client** devices, and then restart the device.
7. Change the run mode of the **Client** devices from **Standalone** back to **Client** mode.

Resolved Issues

- You can now properly restore a Centralized Management configuration from version 8.1 to XCS 9.1 or greater. *[59943]*
- The system now properly notifies you that mail sending must be disabled when you use the "Remove All" function on the Mail Queue page. *[60930]*
- When using the Web Proxy, files that take longer than 20 seconds to scan for viruses are no longer treated as suspicious. *[64536]*
- Line breaks no longer occur in annotations to HTML message parts encoded in quoted-printable characters. *[67287]*
- Timeout errors are less likely to occur during FTP backup operations to an FTP server. *[66264]*
- The FreeBSD Security Advisory FreeBSD-SA-12:02.crypt has been resolved. *[67115]*
- Document contents are now properly saved when you edit and save an existing Phrase List dictionary for Document Fingerprinting. *[68214]*
- The TLS caching process no longer causes mail processing issues. *[62996]*
- Download errors and warnings no longer occur when you try to download certain types of dictionaries. *[68459]*
- You can now properly configure an NTP server using a host name. *[68483]*
- The content of a dictionary is now properly updated by the system when you edit an existing UTF-8 dictionary with the text window. *[68524]*
- The Offload Logs configuration is now properly restored and applied from a backup. *[52320]*
- Tiered administrators can now change their password and user profile settings when they log in to a cluster. *[61694]*
- WatchGuard XCS 770R model platforms no longer experience file system lockups. *[67567]*
- Web Admin UI delays no longer occur when there are a high number of unacknowledged alarms. *[67697]*
- Dictionary files are now properly updated on cluster systems when a dictionary is deleted. *[68100]*
- The Content Scanning engine has been upgraded to provide the latest security improvements for deep content scanning of files and attachments. *[68134]*
- You can now edit the details of large dictionaries that were entered as text when you created the dictionary. *[68135]*
- You can now add 4-letter TLDs to a Domain type dictionary. *[68659]*
- Recipient verification no longer fails when you have the Reject on Missing Addresses option enabled. *[68664]*
- SMTP probe now works properly when mail servers are located behind certain kinds of network devices. *[69179]*
- Processing issues no longer occur with certain types of PDF files. *[69437]*
- Message processing delays no longer occur when using SMTP recipient verification. *[69577]*

Known Issues and Limitations

These are the known issues for this release. Where available, we include a way to work around the issue.

- Words in international dictionaries that use folded characters (for example, ß for ss) are not detected by content scanning when the common unfolded version is found in a message. *[68917]*

> **Workaround**
> When you create your dictionary, add dictionary words for both the folded and common unfolded versions of the characters.

- Internationalized content scanning does not consistently work for HTTP/HTTPS traffic over the Web Proxy. *[69883]*
- SMTP recipient verification rejects valid incoming messages when message sending on the XCS is disabled. *[69732]*
- Document Fingerprinting does not currently support international document capability. *[68819]*
- Content Scanning internationalization does not currently support scanning the mail body for Chinese Simplified (HZ), Korean, and UTF-7 encodings. *[69971]*
- If you uninstall and then reinstall 9.2 Update 4, any dictionaries used for international content scanning may not be applied properly during message processing. *[69975]*

> **Workaround**
> If you uninstall and then reinstall 9.2 Update 4, you must re-upload and apply any dictionaries used for international content scanning.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375